PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-087336
(43)Date of publication of application : 20.03.2003

(51)Int.Cl. H04L 12/66
G06F 13/00
H04L 29/06

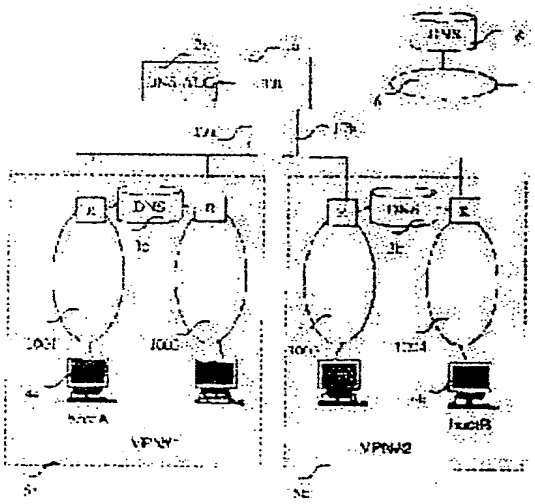
(21)Application number : 2001-274419
(22)Date of filing : 11.09.2001

(71)Applicant : HITACHI LTD
(72)Inventor : INAI HIDENORI
TAKEDA SACHIKO
HAYASHI MASAYA
TAKEUCHI TAKAAKI
SENOO TAKAMITSU

(54) ADDRESS CONVERSION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To solve a problem of a conventional technology that cooperation between the DNS-ALG (Domain Name Service-Application Level Gateway) and the Twice NAT (Network Address Translation) is not scalable because an increased size of the conversion table is required.
SOLUTION: A translator 1a has a communication means with a DNS-ALG 2. The DNS-ALG 2 detects a DNS inquiry to a called party terminal 4b and converts it once into the IPv6. The DNS-ALG 2 converts a called destination virtual IPv6 address resulting from attaching a virtual IPv6 prefix to the real address of the IPv4 acquired from a DNS server 3b of the called party terminal 4b into a called party virtual IPv4. Thus, cooperation of the DNS-ALG of the IPv6 base and the translator 1 can relieve the processing load on the DNS-ALG 2 and reduce a large capacity conversion table. Interconnection is thus attained among a plurality of VPNs without the need for replacing the existing VPN.

図16



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－87336
(P2003－87336A)
(43)公開日　平成15年３月20日(2003.3.20)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード(参考)
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　12/66	Ｅ	５Ｂ０８９
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｂ	５Ｋ０３０
Ｈ０４Ｌ　29/06		Ｈ０４Ｌ　13/00	３０５Ｂ	５Ｋ０３４

審査請求　未請求　請求項の数20　ＯＬ　（全 20 頁）

(21)出願番号　特願2001－274419(P2001－274419)

(22)出願日　平成13年９月11日(2001.9.11)

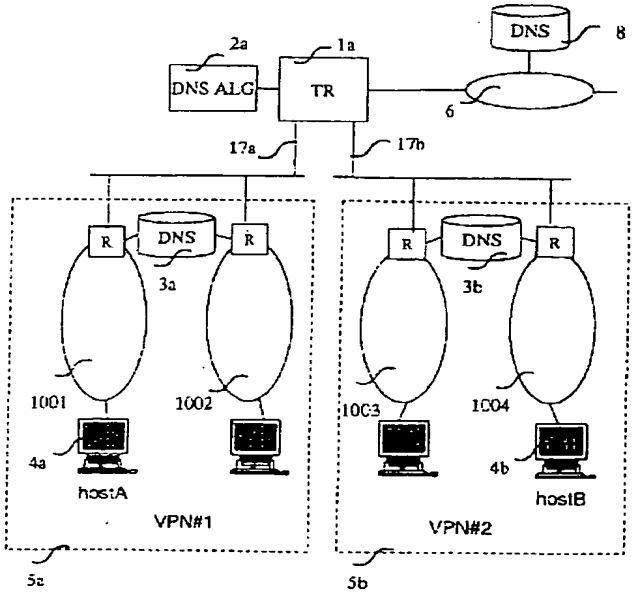
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　井内　秀則
東京都国分寺市東恋ケ窪一丁目280番地
株式会社日立製作所中央研究所内
(72)発明者　武田　幸子
東京都国分寺市東恋ケ窪一丁目280番地
株式会社日立製作所中央研究所内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　アドレス変換方法

(57)【要約】　（修正有）
【課題】DNS-ALGとTwice NATの連携は、変換テーブルが増大するため、スケーラブルではない。
【解決手段】トランスレータ１ａはDNS-ALG２との通信手段を備える。DNS-ALG２は、着側端末４ｂに対するDNS問い合わせを検出し、一度IPv6に変換する。DNS-ALG２は、着側端末４ｂのDNSサーバ３ｂから取得したIPv4の実アドレスに仮想IPv6プレフィックスを付加した着信先仮想IPv6アドレスを着信先仮想IPv4に変換する。
【効果】IPv6ベースのDNS-ALGとトランスレータ１の連携により、DNS-ALG２の処理負荷の軽減と大容量変換テーブルの削減を可能にする。既存のVPNを置きかえることなく、複数のVPN間で相互接続が可能になる。

図16



【特許請求の範囲】

【請求項１】第１のプロトコルPに従う複数の網A１、A2と、第２のプロトコルQに従う網Bと、上記網A１と網Bを接続する第１のアドレス変換装置と、上記網A2と網Bを接続する第２のアドレス変換装置と、サーバ装置を有する通信網におけるアドレス変換方法であって、

上記第１及び第２のアドレス変換装置はプロトコルP、Qを相互に変換する手段と、上記サーバ装置との通信手段と、上記サーバ装置と連携してプロトコルPでのアドレスとプロトコルQでのアドレスの対応関係を含む変換情報を作成する手段を有し、上記サーバ装置は、上記アドレス変換装置がプロトコルP、Qを相互に変換するために必要な変換情報と、上記変換情報を作成するために他のサーバ装置と通信する手段を有し、

上記第１のアドレス変換装置が上記変換情報を参照してプロトコルPとプロトコルQを相互に変換したのち、上記第２のアドレス変換装置がプロトコルQとプロトコルPを相互に変換することにより、プロトコルPに従う網A1がプロトコルPに従う網A2と通信することを特徴とするアドレス変換方法。

【請求項２】あるプロトコルPに従う網と上記プロトコルPと異なるプロトコルQに従う網とを接続するアドレス変換装置において、プロトコルP、Qを相互に変換する手段と、プロトコルP、Qを相互に変換するために必要な情報を有するサーバ装置と通信する手段と、上記サーバ装置と連携してプロトコルPでのアドレスとプロトコルQでのアドレスの対応関係を含む変換情報を作成する手段と、プロトコルP、Qを相互変換する際に上記作成した変換情報を参照することを特徴とするアドレス変換装置。

【請求項３】あるプロトコルPに従う複数の網と上記プロトコルPと異なるプロトコルQに従う網とを、プロトコルP、Qを相互に変換する複数のアドレス変換装置で接続する通信網におけるサーバ装置において、上記アドレス変換装置においてプロトコルP、Qを相互に変換するために必要な変換情報と、上記変換情報を作成するために他のサーバ装置と通信する機能と、上記アドレス変換装置にプロトコルPでのアドレスとプロトコルQでのアドレスの対応関係を含む変換情報の作成を要求する手段を備えるサーバ装置。

【請求項４】あるプロトコルＰに従う複数の網A１、A2をアドレス変換装置で接続する通信網において、

アドレス変換装置はプロトコルPを内部でプロトコルQに相互に変換する機能と、サーバ装置と通信するために必要な情報と通信手段と、上記サーバ装置と連携して、プロトコルPでのアドレスとプロトコルQでのアドレスの対応関係を含む変換情報を作成する機能とを備え、上記サーバ装置は、上記アドレス変換装置においてプロトコルP、Qを相互に変換するために必要な変換情報と、上記プロトコルPに従う網対応にプロトコルQに従うアドレスと、上記変換情報を作成するために他のサーバ装置、もしくは、上記サーバ装置の別のアドレスと通信する機能を備え、

プロトコルPに従う網A1からプロトコルPに従う網A2への通信は、上記アドレス変換装置が上記変換情報を参照してプロトコルPに従うアドレスからプロトコルQに従うアドレスに変換し、変換されたプロトコルQに従うアドレスをさらにプロトコルPに従うアドレスに変換することを特徴とする通信網。

【請求項５】上記アドレス変換装置が上記プロトコルPに従う複数の網をレイヤ２の情報により識別する機能をさらに有し、

上記アドレス変換装置が通信要求を受信するとレイヤ２の情報によりプロトコルPに従う網を特定し、プロトコルPからプロトコルQに変換することを特徴とする請求項４に記載の通信網。

【請求項６】上記プロトコルPに従う複数の網が、多重装置に接続され、上記多重装置と上記アドレス変換装置が複数の回線で接続され、

上記多重装置が上記プロトコルPに従う網をレイヤ２の情報により識別する機能を備え、

上記多重装置が上記プロトコルPに従う網から通信要求を受信するとレイヤ２の情報によりプロトコルPに従う網を特定し、対応する回線を用いて、上記アドレス変換装置に通信要求を送信する請求項4に記載の通信網。

【請求項７】あるプロトコルＰに従う複数の網が異なるアドレス変換装置に接続され、アドレス変換装置がプロトコルQに従う網に接続される通信網における請求項４に記載の通信網。

【請求項８】あるプロトコルPに従う複数の網接続するアドレス変換装置において、

プロトコルPを内部でプロトコルQに相互に変換する機能と、

サーバ装置と通信するために必要な情報と通信手段と、上記プロトコルPに従う網対応にプロトコルQに従うアドレスと、プロトコルP、Qを相互に変換するために必要な変換情報と、上記変換情報を作成するために他のサーバ装置、もしくは、上記サーバ装置の別のアドレスと通信する機能を備えるサーバ装置と連携して、プロトコルPでのアドレスとプロトコルQでのアドレスの対応関係を含む変換情報を作成する機能を備えるアドレス変換装置。

【請求項９】上記プロトコルPに従う複数の網をレイヤ２の情報により識別する機能をさらに備え、

通信要求を受信するとレイヤ２の情報によりプロトコルPに従う網を特定し、プロトコルPからプロトコルQに変換する手段を備える請求項8に記載のアドレス変換装置。

【請求項１０】あるプロトコルＰに従う複数の網をアドレス変換装置で接続する通信網において、

上記アドレス変換装置は、内部でプロトコルPをプロト

コルQに相互に変換する機能と、サーバ装置と通信するために必要な情報と通信手段を備え、
上記プロトコルPに従う網対応にプロトコルQに従うアドレスと、プロトコルP、Qを相互に変換するために必要な変換情報と、上記変換情報を作成するために他のサーバ装置、もしくは、上記サーバ装置の別のアドレスと通信する手段と、
上記アドレス変換装置にプロトコルPでのアドレスとプロトコルQでのアドレスの対応関係を含む変換情報の作成を要求する手段を備える通信網。
【請求項１１】あるプロトコルPに従う複数の網が異なるアドレス変換装置に接続され、アドレス変換装置がプロトコルQに従う網に接続される通信網における請求項10に記載の通信網。
【請求項１２】あるプロトコルPに従う複数の網をアドレス変換装置で接続する通信網において、
アドレス変換装置は、内部で上記プロトコルPをプロトコルQに相互に変換する機能と、サーバ装置と通信するために必要な情報と通信手段を備え、
上記プロトコルP、Qを相互に変換するために必要な変換情報と、
上記変換情報を作成するために、あるプロトコルPに従う網の識別情報とプロトコルPに従う網に属するサーバ装置に対して付与されたプロトコルQに従うアドレスの対応関係を管理し、あるプロトコルPに従う網の名前解決要求を受信すると、上記対応関係を参照して他のサーバ装置と通信する手段と、
上記アドレス変換装置にプロトコルPでのアドレスとプロトコルQでのアドレスの対応関係を含む変換情報の作成を要求する手段を備えるサーバ装置。
【請求項１３】あるプロトコルＰに従う複数の網が異なるアドレス変換装置に接続され、アドレス変換装置がプロトコルQに従う網に接続される通信網における請求項12に記載のサーバ装置。
【請求項１４】あるプロトコルPに従う複数の網をアドレス変換装置で接続する通信網において、
アドレス変換装置はプロトコルPを内部でプロトコルQに相互に変換する機能と、サーバ装置と通信するために必要な情報と通信手段と、上記サーバ装置と連携して、プロトコルPでのアドレスとプロトコルQでのアドレスの対応関係を含む変換情報を作成する機能を備え、上記サーバ装置は、上記アドレス変換装置においてプロトコルP、Qを相互に変換するために必要な変換情報と、
上記変換情報を作成するために、あるプロトコルPに従う網の識別情報とプロトコルPに従う網に属するサーバ装置に対して付与されたプロトコルQに従うアドレスの対応関係と、あるプロトコルPに従う網の名前解決要求を受信すると、上記対応関係を参照して他のサーバ装置と通信する手段と、
上記アドレス変換装置にプロトコルPでのアドレスとプロトコルQでのアドレスの対応関係を含む変換情報の作成を要求する手段を備え、
プロトコルPに従う網A1からプロトコルPに従う網A2への通信は、上記アドレス変換装置が上記変換情報を参照してプロトコルPに従うアドレスからプロトコルQに従うアドレスに変換し、変換されたプロトコルQに従うアドレスをさらにプロトコルPに従うアドレスに変換することを特徴とするアドレス変換方法。
【請求項１５】あるプロトコルＰに従う複数の網が異なるアドレス変換装置に接続され、アドレス変換装置がプロトコルQに従う網に接続される通信網における請求項14に記載のアドレス変換方法。
【請求項１６】第１の網と、該第１の網と通信可能な第２の網と、該第２の網と通信可能な第３の網と、上記第１の網と第２の網を接続する第１のアドレス変換装置と、上記第２の網と第３の網を接続する第２のアドレス変換装置とを有し、
上記第１のアドレス変換装置は、上記第１の網で使われているアドレスに上記第１の網を示すプレフィックスを付加した第１仮想アドレスを、上記第２の網を介して上記第２のアドレス変換装置に送り、
上記第２のアドレス変換装置は、上記第１仮想アドレスを上記第３の網で使われていないアドレスである第２仮想アドレスに変換して、上記第３の網に送り、上記第１仮想アドレスと上記第２仮想アドレスとの対応情報を記憶することを特徴とする情報網。
【請求項１７】上記第３の網から送られてきた上記第２仮想アドレスを、上記対応情報に基づいて上記第１仮想アドレスに変換し、該第１仮想アドレスから上記プレフィックスを削除して、上記第１の網に送ることを特徴とする請求項１６記載の情報網。
【請求項１８】上記第１の網は第１のプロトコルに従い、上記第２及び第３の網は第２のプロトコルに従うことを特徴とする請求項１７記載の情報網。
【請求項１９】第１の網と第２の網の間に配置され、該第１の網と第２の網の間の通信を仲介する通信装置であって、
上記第１の網から送られてきた上記第１の網で使われている元アドレスを受信し、該元アドレスにプレフィックスを付加した第１仮想アドレスを形成し、該第１仮想アドレスを上記第２の網に送出し、
上記第２の網から送られてきた上記第１仮想アドレスを受信し、該第１仮想アドレスからプレフィックスを削除して元アドレスを形成し、該元アドレスを上記第１の網に送出することを特徴とする通信装置。
【請求項２０】上記第２の網から送られてきた第１アドレスを、上記第１の網で使われていない第２アドレスに変換し、上記第１の網に送出し、
上記第１アドレスと第２アドレスの関連を変換情報として保持し、

上記第１の網から送られてきた第２アドレスを、上記変換情報にもとづいて上記第１アドレスに変換し、
該第１アドレスを上記第２の網に送出することを特徴とする請求項１９記載の通信装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は同一のプロトコルに従う網、あるいは、異なるプロトコルに従う網を相互接続する方式に関する。
【０００２】
【従来の技術】例えばプライベート網どうしをインターネットで接続し、ひとつのVPN(VirtualPrivate Network)として見せる技術として、Twice NAT(Network Address TRanslation)技術を使う方法(http://www.ietf.org/rfc/rfc2663.txtのpp12-13参照)や、トンネル技術を使う方法（http://www.ietf.org/rfc/rfc2663.txtのpp22参照）が知られている。いずれも基本的にIPパケットのヘッダ情報をIPv4とIPv4とで相互に変換する。例えば基本的なNATは、プライベートIPv4アドレスとパブリックIPv4アドレスの変換を行う。NATを２つ直列に接続した、いわゆるTwice NAT技術を実装したルータはTwice NATルータと呼ばれる。従来の基本NAT、双方向NATでは、送信元アドレス、もしくは着信先アドレスのどちらか一方を書き換えていたが、Twice NAT技術では、Twice NATルータで接続された二つの領域間をデータグラムが通過する時点で、送信元アドレスと着信先アドレスの両方を書き換える。Twice NATは、プライベートネットワーク内のアドレス空間とパブリック空間のアドレス空間が衝突している場合に使われることが多い。あるサイトのアドレス付けを誤って他のサイトのパブリックアドレスをつけてしまった場合、あるプロバイダからアドレスをもらっていたが、他のプロバイダに乗り換えた後もしばらくは、以前のプロバイダから割り当ててもらったアドレスを使い続け、そのプロバイダが別ユーザに対して同じアドレスを割り当ててしまった場合に、アドレス衝突が発生する。アドレス衝突を解決するためには、Twice NATは以下のように動作する。プライベート領域内のHost-Aがパブリック領域内のHost-Xと通信をはじめる場合には、Host-A はHost-XのDNSアドレス問い合わせパケットを送信する。DNS-ALG(Domain Name Service - Application Level Gateway)がこのパケットを捕捉し、かつHost-Xに対するアドレスをプライベート領域内でルーティング可能なアドレス（Host-XPRIME）に変換してHost-Aに返す。DNSアドレス解決が終了したらHost-AはHost-XPRIMEとの間で通信を開始する。このパケットがTwice NATを通過する時点で、送信元アドレスがNATの持つアドレスに書き換えられ、着信先アドレスはHost-Xに書き換わる。Host-Xからの返信パケットもこれと同様の変換が行われる。上記DNS-ALGの動作詳細については、http://www.ietf.orf/rfc/rfc2693.txtに詳細が記載されている。Twice NATを使用する方法は、インターネットを介して多数のホストどうしで通信する場合に、大容量の変換テーブルが必要になる。特定のIPアドレスを使うアプリケーションが多い場合には、上記のようにDNSアドレス問い合わせをトリガにしたNATによるダイナミックなアドレス変換ができないという問題がある。上記の問題点を解決するために、NAT技術ではなくトンネル技術を用いて二つの領域を相互接続する方法がある。トンネル技術を用いる方法は、接続対象になっている二つの網内の端末が同一のアドレスを持つ場合には、同一のアドレスを有する端末間では通信ができない、異なる接続する二つの領域が同一のサブネットを持たないといけないという制限がある。しかしながら、Twice NAT使用時のように大容量の変換テーブルを持つ必要はないので、インターネットを介して同一のサブネット空間を共有するPrivate VLAN(Virtual LAN)どうしを相互接続する技術としてはトンネル技術が使われることが多い。以上の例は、ある端末が属する網と通信相手の端末が属する網の通信プロトコルが同一の場合に使われる技術である。ある端末が属する網と通信相手の端末が属する網の通信プロトコルが異なる場合には、例えばプロトコルとしてIPv4を用いる網(以下IPv4網と呼ぶ)とInternet Protocol version 6を使用する網(以下IPv6網と呼ぶ)を接続する変換方式としてNAT-PT(http://www.ietf.org/rfc/rfc2766.txtのpp6-18、およびrfc2765.txtのpp9-22参照)、SOCKS64(http://search.ietf.org/internet-drafts/draft-ietf-ngtRans-socks-gateway-05.txt参照)等が知られている。いずれも基本的にIPパケットのフォーマットをIPv4とIPv6とで相互に変換する。例えば、IPv4アドレスとIPv6アドレスの変換を行う。この変換を行う装置を以下トランスレータと呼ぶ。トランスレータでは変換のために、変換の前にIPv4アドレスとIPv6アドレスの対応関係を作成し、保持しておく必要がある。この対応関係を通信が発生するたびに動的に作成する場合に、そのきっかけとしてDNS(ドメインネームシステム)の名前解決が利用される(アスキー出版、インターネットRFC事典、pp323-329を参照)。DNSはウェブのURLのような人間にわかりやすい名前(文字列)を、IPアドレスに変換するシステムである。以下名前をIPアドレスに変換する操作を名前解決と呼ぶ。今日ではインターネット上のほぼすべてのアプリケーションがこのDNSを利用して通信相手のIPアドレスを取得している。NAT、及びトランスレータはこの事実を利用し、通信開始にあたってやり取りされるDNSのメッセージを常に監視しており、名前解決の要求メッセージを変換情報(IPアドレスの対応関係等)を作成するきっかけとする。具体的には、IPv6端末がある名前について名前解決を行ったとき、その応答であるIPアドレスがIPv4だった場合、このIPv4アドレスをIPv6アドレスに書き換えてIPv6端末に送り返す。そして、書き換える前のIPv4アドレスと書き換えたIPv6アドレスを対応付ける。つ

まりDNS-ALGは名前解決の応答メッセージを横取りして書き換え、この書き換える前と書き換えた情報をもとに変換情報を作成する。ここで動的に作成された変換情報は一時的なものであるから、通信が終了すると廃棄される。DNS-ALGが保持する、IPv4アドレスとIPv4アドレスの対応関係、若しくはIPv4アドレスとIPv6アドレスの対応関係は通信終了とともに廃棄され、通信ごとに異なるものが使用される。すなわち、名前解決の応答メッセージを書き換える内容が通信ごとに異なる。したがって、名前解決を要求した端末から見ると、同じ名前に対して異なるIPアドレスを取得することとなる。

【０００３】このように、DNS-ALGとトランスレータの連携は、インターネット上のほぼすべてのアプリケーションがこのDNSを利用して通信相手のIPアドレスを動的に取得している状況において、IPv6ネットワークとIPv4ネットワークを接続するために必須の技術である。また、DNS-ALGとTwice NATの連携は、パブリックアドレスの移行時に発生するIPv4プライベートアドレスの競合問題を解決する技術である。

【０００４】

【発明が解決しようとする課題】上述した通り、トンネル方式によるVPNの相互接続は、IPアドレスの衝突に対処できないという課題がある。また、DNS-ALGとTwice NATの連携は、パブリックアドレスの移行時に発生するIPv4プライベートアドレスの競合問題を解決する技術である。しかし、DNS-ALGとTwice NATの連携は、アドレス変換テーブルが大きく、スケーラブルでないという課題がある。一般的に、VPN間の相互接続は、VPNのエッジにDNS-ALGとTwice NATを設置し、実現することが多い。しかし、相互接続するVPNの数が多い場合、アドレス変換テーブルが大きくなるため、サービスの提供が困難であるという課題がある。本発明の目的は、ある端末が属する網と通信相手の端末が属する網の通信プロトコルが同一の場合に、両網のアドレス空間が衝突した場合にも、両方の端末どうしの通信を可能にすることにある。本発明の他の目的は、ある端末が属する網と通信相手の端末が属する網の通信プロトコルが異なる場合には、基本トランスレーションによって、両方の端末どうしの通信を可能にする、スケーラブルで実用的なアドレス変換装置を提供することにある。

【０００５】本発明はIPv6ベースのDNS-ALGとTwice NAT-PTの連携によって、従来のTwice NATによるアドレス変換で必要な変換情報を動的に作成する場合に必要であった、着側の端末に対する仮想アドレスを生成するDNS-ALGの処理負荷の軽減と大容量変換テーブルの削減を可能にする。

【０００６】本発明によるIPv6ベースのDNS-ALGとTwice NAT-PTをプロバイダが一括管理し、トランスレータに複数のVPNを収容すれば、既存のVPNを置きかえることなく、複数のVPN間での相互接続が可能になる。

【０００７】

【課題を解決するための手段】従来の、NAT-PTに代表されるプロトコル変換方式に加え、少なくとも以下の２点の手段を備える。すなわち、①複数のトランスレータがもつ、IPv4アドレスとIPv6アドレスの対応関係に代表されるアドレス変換に必要な変換情報を管理するDNS-ALG装置を備え、②各トランスレータは前記DNS-ALG装置と通信を行うためのプロトコルを備える。

【０００８】Twice NAT-PTによるアドレス変換で必要な変換情報を動的に作成するため、DNS-ALG装置は、発側の端末からの送信される着側端末に対するDNS問い合わせを、装置の内部では一度IPv6に変換する。DNS-ALG装置は、着側のIPv4 DNSサーバにおける問い合わせで取得したIPv4の実アドレスに仮想IPv6プレフィックスを付加したIPv6アドレスを着側の端末に対する仮想IPv6アドレスとして使用する。仮想IPv6アドレスを仮想IPv4アドレスに変換し、発側端末に通知する。この方式をとることによって、従来のTwice NAT方式と比較すると、変換回数が一回少なくなると同時に変換テーブルのサイズを小さくすることができる。さらに、③各トランスレータはL2情報を活用してプロトコル変換を行う手段を備えてもよい。IPアドレス以外にもMACアドレスに代表されるL2情報を用いたプロトコル変換を行う手段を備えることによって、１つの物理回線上に複数のVPNを多重することが可能になる。このような発明を適用した情報網は、第１の網と、第１の網と通信可能な第２の網と、第２の網と通信可能な第３の網と、第１の網と第２の網を接続する第１のアドレス変換装置と、第２の網と第３の網を接続する第２のアドレス変換装置とを有し、第１のアドレス変換装置は、第１の網で使われているアドレスに第１の網を示すプレフィックスを付加した第１仮想アドレスを、第２の網を介して第２のアドレス変換装置に送り、第２のアドレス変換装置は、第１仮想アドレスを第３の網で使われていないアドレスである第２仮想アドレスに変換して第３の網に送り、第１仮想アドレスと第２仮想アドレスとの対応情報を記憶する。また、第３の網から送られてきた第２仮想アドレスを、対応情報に基づいて第１仮想アドレスに変換し、第１仮想アドレスからプレフィックスを削除して、第１の網に送る。この場合、第１の網は第１のプロトコルに従い、第２及び第３の網は第２のプロトコルに従うこととしてもよい。また、変換されるアドレスは、送信元アドレスまたは送信先アドレスとしてもよい。

【０００９】このような網に用いられる通信装置としては、第１の網と第２の網の間に配置され、第１の網と第２の網の間の通信を仲介する通信装置であって、第１の網から送られてきた第１の網で使われている元アドレスを受信し、元アドレスにプレフィックスを付加した第１仮想アドレスを形成し、第１仮想アドレスを第２の網に送出し、第２の網から送られてきた第１仮想アドレスを

受信し、第１仮想アドレスからプレフィックスを削除して元アドレスを形成し、元アドレスを第１の網に送出する。

【００１０】また、他の通信装置は、第２の網から送られてきた第１アドレスを、第１の網で使われていない第２アドレスに変換し、第１の網に送出し、第１アドレスと第２アドレスの関連を変換情報として保持し、第１の網から送られてきた第２アドレスを、変換情報にもとづいて第１アドレスに変換し、第１アドレスを第２の網に送出する。

【００１１】

【発明の実施の形態】本発明の第１の実施の形態を図面を用いて説明する。

【００１２】図１は、本発明によるVPN間接続サービスを提供するネットワークの構成例を示す。VPN間接続サービスを提供するネットワークは、VPN５とIP網６から構成される。VPN５は、DNSサーバ３を備える。VPN5aは、例えば企業の拠点（１００１、１００２）を仮想的に相互に接続する。本実施例では、VPN５は、IPv4プライベートアドレスを利用する。１つのVPN内においてはIPアドレスは重複しないが、異なるVPNの間でIPアドレスは重複してもよい。IP網６はDNSサーバ８を備える。本実施例では、IP網６はIPv6アドレスを利用する。

【００１３】VPN５とIP網６は、トランスレータ１（TR）で接続する。トランスレータ１は、IPv6アドレスとIPv4アドレスの変換機能と、DNS-ALG２と通信する手段を備える。DNS-ALG２は、複数のトランスレータがもつIPv4アドレスとIPv6アドレスの対応関係に代表されるアドレス変換に必要な変換情報を管理し、DNSの問い合わせやその返信のパケットの中身を書き換える手段を備える。第１の実施の形態において、DNS-ALG２は、VPN５毎に存在する。

【００１４】図２は、トランスレータ１の構成例を示す。トランスレータ１は、回線（17a、17b、17c、17n）を収容するインタフェース部（IF）（16a、16b、16c、16n）と、メモリ14と、CPU15とを、スイッチまたはバス18で接続する構成となっている。メモリ14は、アドレスの変換に必要な情報１１やデータパケットを変換するためのプログラム１３や、DNS-ALG２からの変換エントリ登録要求を処理するためのプログラム１２が格納されている。変換情報記憶部１１は、図９に示す仮想プレフィックス管理テーブル３００と図１１に示す変換情報テーブル５００を備える。

【００１５】図９は、仮想プレフィックス管理テーブル３００のテーブル構成を示す。本テーブルは、トランスレータ１の回線番号ごとに生成された複数のエントリ（３００－１～３００－ｎ）からなる。各エントリは、回線番号３０１対応に、仮想プレフィックス３０２と、変換情報テーブル５００へのポインタ３０３を定義する。

【００１６】図１１は、変換情報テーブル５００のテーブル構成を示す。本テーブルには、IPv4アドレス５０１とIPv6アドレス５０２の対応関係が格納される。本テーブルは、VPN毎に生成され（５１０、５２０、５３０）、VPNを収容するトランスレータ１の変換情報記憶部１１に格納される。例えば、図１において、VPN#1変換情報テーブル５１０はトランスレータ１ａに、VPN＃3変換情報テーブル５３０はトランスレータ１ｂに格納される。

【００１７】図２へ戻りトランスレータ１の説明を続ける。変換エントリ登録処理１２は、変換情報登録要求を処理し、IPアドレスの対応情報を変換情報記憶部１１の変換情報テーブル５００に格納する。データパケット変換・処理部１３は、IPv4パケットを受信すると変換情報記憶部１１を検索し、IPv6アドレスをIPv4アドレスに書き換える。また、データパケット変換・処理部１３は、IPv6パケットを受信すると、変換情報記憶部１１を検索し、IPv4アドレスをIPv6アドレスに書き換える。このとき、IPアドレスのほかにもさまざまな情報を書き換えることが可能である。図４にIPv4パケットフォーマットを示す。図５にIPv6パケットのフォーマットを示す。変換の際にはIPアドレスだけでなく、このフォーマットも変換する。

【００１８】図３は、DNS-ALG２の構成例を示す。DNS-ALG２は、回線(24a、24b)を収容するインタフェース部（IF）（23a、23b）と、メモリ22と、CPU21とを、バス25で接続する構成となっている。

【００１９】図１４と図１５に示すシーケンスに従って、図１におけるVPN５ａの端末４ａがVPN５ｃの端末４ｃと通信する場合について説明する。通信開始にあたり、端末４ａは端末４ｃの名前(hostCとする)のアドレスを得るため、DNSサーバ３ａに対してDNS問い合わせを行う（１０１）。DNS問い合わせのパケットフォーマットを図６に示す。図６に示すように、QNAME（４２１）に名前hostCが、QTYPE（４２２）に資源レコードのタイプ”A”が記載される。図１４に戻り説明を続ける。DNSサーバ3ａはこの名前hostCに対応するIPアドレスを知らないため、次のDNSサーバ（DNS-ALG２ａ）に対してDNS問い合わせを行う（１０２）。

【００２０】DNS-ALG２ａは、名前hostCに対するIPアドレスを知らない場合、図１２、１３に示す処理ルーチン６０を起動する。DNS問い合わせのQTYPEが“A”の場合、DNS-ALG２ａはQTYPEを“AAAA”に変換する（６２、１０３）。DNS-ALG２ａは変換したDNS問い合わせを次のDNSサーバ８に送信し（６３、１０４）、DNS応答を待つ（６４）。DNSサーバ８は、次のDNSサーバ（DNS-ALG２ｂ）にDNS問い合わせを送信する（１０５）。DNS-ALG２ｂは、名前hostCに対するIPアドレスを知らない場合、図１２、１３に示す処理ルーチン６０を起動する。DNS問い合わせのQTYPEが“AAAA”の場合、QTYPEを“A”に

変換する（８１、１０６）。DNS-ALG２ｂは変換したDNS問い合わせを次のDNSサーバ３ｃに送信し（８２、１０７）、DNS応答を待つ（８３）。DNSサーバ３ｃは、名前hostCに対するIPv4アドレス“ｃ”を応答する（８４、１０８）。

【００２１】図７にDNSサーバ３ｃからの DNS応答パケットのフォーマットを示す。図７の４３、４４、４５の詳細フォーマットを図８に示す。NAME（５１）に名前hostC、RDATA（５４）にIPアドレス“ｃ”が記載される。図１４を参照すると、DNS-ALG２ｂは以後の変換のためにIPv4アドレス“ｃ”をIPv6アドレス“γ＋ｃ”に書き換える。このIPv6アドレスは、VPN5cに対して割り当てられる仮想的なIPv6プレフィックス（γ）＋IPv4アドレス（ｃ）で構成される（１０９）。以降、このアドレスを「着信先仮想IPv6アドレス」と呼ぶ。DNS-ALG２ｂは、DNS応答のTYPE（５２）を“A”から“AAAA”に変換し、RDATA（５４）に“γ＋ｃ”を設定したDNS応答をDNSサーバ８に送信する（８５、１１０）。DNSサーバ８は、DNS-ALG２ａに名前hostCに対する着信先仮想IPv6アドレス“γ＋ｃ”を応答する（６５、１１１）。DNS-ALG２ａは、以後の変換のために、このIPv6アドレス“γ＋ｃ”をIPv4アドレスｃ’に変換する（１１２）。このIPv4アドレスは名前hostCに対する仮想的なアドレスで、VPN５ａで使用されていないIPアドレスの集合から選ぶ。以降、このアドレスを「着信先仮想IPv4アドレス」と呼ぶ。DNS-ALG２ａは、DNS応答のTYPE（５２）を“AAAA”から“A”に変換し、RDATA（５４）に着信先仮想IPv4アドレス“ｃ’”を設定したDNS応答をDNSサーバ３ａ経由で端末４ａに送信する（６６、１１５、１１６）。このとき、γ＋ｃとｃ’の対応付け変換規則を作成し、トランスレータ１ａに送信する（６７、１１３）。トランスレータ１ａは、変換規則を変換情報記憶部１１内のVPN≒１変換情報テーブル５１０に記憶し、DNS-ALG２ａに応答を送信する（１１４）。

【００２２】DNS応答を受信した端末４ａは端末４ｃへ向けてIPパケットの送信を始める。これらのパケットの着信先アドレスはｃ’、送信元アドレスは端末のIPv4アドレスａである（１３１）。

【００２３】トランスレータ１ａは、このパケットが到着するとデータパケット変換・処理部１３に送る。ここでは、変換情報記憶部１１にデータを受信した回線の番号と着信先アドレスｃ’で検索をかける。すると、ステップ１１３で準備したエントリが変換情報テーブル５１０に見つかるため、着信先アドレス“ｃ’”を“γ＋C”に変換する。送信元アドレスは、データを受信した回線番号に対応する仮想的なIPv6プレフィックスαを付加した「送信元仮想IPv6アドレス」“α＋ａ”に書き換える（１３２）。トランスレータ１ａは着信先アドレスに“γ＋ｃ”、送信元アドレスに“α＋ａ”をそれぞれ設定したパケットを送信する（１３３）。トランスレータ１ｂはこのパケットをデータパケット変換・処理部１３に送る。ここでは、着信先アドレスから仮想IPv6プレフィックスγを削除する。送信元アドレス“α＋ａ”をVPN５ｃの内部で一意に識別するため、IPv4アドレス“ａ１’”に変換する。このIPv4アドレスは、送信元アドレス“α＋ａ”に対する仮想的なアドレスで、VPN５ｃの内部で使用されていないIPアドレスの集合から選ぶ。以降、このアドレスを「送信元仮想IPv4アドレス」と呼ぶ。

【００２４】トランスレータ１ｂは、“α＋ａ”と“ａ１’”の対応付け変換規則を作成し、変換情報記憶部１１のVPN≒３変換情報テーブル５３０に記憶する（１３４）。端末４ｃが着信先アドレスに“ｃ”、送信元アドレスに“ａ１’”を設定したパケットを受信する（１３５）。端末４ｃは、端末４ａへ向けて着信先アドレス“ａ１’”、送信元アドレス“ｃ”を設定したIPパケットを送信する（１３６）。トランスレータ１ｂではこのパケットが到着するとデータパケット変換・処理部１３に送る。ここでは、変換情報記憶部１１にデータを受信した回線の番号と着信先アドレス“ａ１’”で検索をかける。すると、ステップ１３４で準備したエントリが変換情報テーブル５３０に見つかるため、着信先アドレスを“ａ１’”を“α＋ａ”に変換する。送信元アドレスは、データを受信した回線番号に対応する仮想的なIPv6プレフィックスγを付加した送信元仮想IPv6アドレス“γ＋ｃ”に書き換える（１３７）。トランスレータ１ｂは着信先アドレスに“α＋ａ”、送信元アドレスに“γ＋ｃ”を設定したパケットを送信する（１３８）。

【００２５】トランスレータ１ａは、このパケットが到着するとデータパケット変換・処理部１３に送る。ここで、着信先アドレスから仮想IPv6プレフィックスαを削除する。変換情報記憶部１１に着信先アドレスの仮想IPv6プレフィックス“α”と送信元アドレス“γ＋c”で検索をかける。すると、さきに準備したエントリが変換情報テーブル５１０に見つかるため、送信元アドレスを“γ＋ｃ”から“c’”に変換する（１３９）。

【００２６】端末４ａは着信先アドレスに“ａ”、送信元アドレスに“ｃ’”を設定したパケットを受信する（１４０）。

【００２７】本発明の実施の形態によれば、トランスレータ１とDNS-ALG２が連携し、IP網6の仮想IPv6プレフィックスを活用することにより、プライベートIPv4アドレスを有するVPN間で相互通信を行うことが可能になる。

【００２８】本発明の第２の実施の形態を図面を用いて説明する。

【００２９】図１６は、本発明の第2の実施例の網構成を示す。図１と比較すると、図１６の網構成は「VPN５のDNSサーバ３とDNS-ALG２の通信がトランスレータ１を経由する」こと、「VPNの相互通信において、DNS-ALG２が次に問い合わせるDNSサーバに、上記DNS-ALG２内の別

IPv6アドレスが設定されている」ことを特徴とする。

【００３０】本実施例において、DNS-ALG２は、トランスレータ１に接続されるVPN対応にIPv6アドレスを有するマルチホームノードである。本実施例におけるDNS-ALG２ａは、次に問い合わせるDNSサーバがDNS問い合わせを送信したVPNに存在しない場合は、次に問い合わせるDNSサーバのアドレス情報として、DNS-ALG２ａの他のIPv6アドレスが記憶されている。次に問い合わせるDNSサーバがDNS問い合わせを送信したVPN内に存在する場合は、次に問い合わせるDNSサーバのアドレス情報として、そのVPN内に存在するDNSサーバの仮想IPv6アドレスが記憶されている。この仮想IPv6アドレスは、“仮想プレフィックス＋各VPNにおいて、DNSサーバに割り当てられたIPv4アドレス”で構成される。

【００３１】本実施例におけるトランスレータ１は、VPN毎のDNS-ALGアドレス変換情報と、DNSのメッセージを含むパケットを監視する機能と、DNSのメッセージを含むパケットのアドレス変換機能をさらに備える。VPN毎のDNS-ALGアドレス変換情報は、VPN対応にDNS-ALGのIPv6アドレスとVPNの内部でDNS-ALGを識別するためDNS-ALGに割り当てられた仮想IPv4アドレスとの対応関係を管理する。

【００３２】図１７と図１８に示すシーケンスに従って、図１６のVPN５ａに存在する端末４ａがVPN５ｂに存在する端末４ｂと通信する場合について説明する。VPN５ａとVPN５ｂは、トランスレータ１ａに接続される。VPN５ａとトランスレータ１ａの間で送受信するパケットのアドレス変換と、VPN５ｂとトランスレータ１ａの間で送受信するパケットのアドレス変換は、トランスレータ１ａで行われる。図１７と図１８において、VPN５ａとトランスレータ１ａの間のアドレス変換機能をTR-O、VPN５ｂとトランスレータ１ａの間のアドレス変換機能をTR-Tと記載する。

【００３３】図１４と図１７の主な差分は、「トランスレータ１ａがDNSのメッセージを含むパケットのアドレスを変換する」ことと、「DNS-ALG２ａのIPv6アドレスがVPN毎に異なる」ことである。

【００３４】以下、図１７と図１８について、詳細に説明する。端末４ａは端末４ｂの名前(host Bとする)を解決するためにDNSサーバ３ａに対してDNS問い合わせを行う（１５１）。DNSサーバ３ａ（IPv4アドレス“da4”）は、この名前host Bに対応するIPアドレスを知らないため、次のDNSサーバ（DNS-ALG２ａ、仮想IPv4アドレス“pa4”）に対してDNS問い合わせを行う（１５２）。

【００３５】トランスレータ１ａのTR-Oは、DNSのメッセージを含むパケットを検出し、パケットを変換する（１５３）。着信先アドレスは、トランスレータ１ａが備えるDNS-ALGアドレス変換情報を用いて、DNS-ALG２ａのVPN５a用のIPv6アドレス”α６”に変換する。送信元アドレスは、仮想プレフィックス管理テーブル300を参照し、VPN５ａ用の仮想IPv6プレフィックス“α”を付加する。トランスレータ１ａのTR-Oは、アドレスを変換したDNS問い合わせパケットをDNS-ALG２ａに送信する（１５４）。

【００３６】DNS-ALG２ａは、名前host Bに対するIPアドレスを知らない場合、前記処理ルーチン６０により、DNS問い合わせを変換し（１５５）、DNS問い合わせを転送する（１５６）。DNS問い合わせの転送先には、DNS-ALG２ａに付与された別のIPv６アドレス（VPN５ｂ用のIPv6アドレス“β６”）が設定されている。

【００３７】VPN５ｂ用のIPv6アドレス“β６”宛のDNS問い合わせを受信したDNS-ALG２ａは、名前host Bに対するIPアドレスを知らない場合、前記処理ルーチン６０により、変換したDNS問い合わせを次のDNSサーバ３ｂ（仮想IPv６アドレス“β＋db4”）に送信する（１５７、１５８）。

【００３８】トランスレータ１ａのTR-Tは、DNSのメッセージを含むパケットを検出し、パケットを変換する（１５９）。着信先アドレスから、仮想プレフィックスβを削除する。送信元アドレスは、トランスレータ１ａが備えるDNS-ALGアドレス変換情報を用いて、VPN5b用のDNS-ALG2aのIPv6アドレス“β６”に対する仮想IPv4アドレス“pb4”に変換する。トランスレータ１ａのTR-Tは、アドレスを変換したパケットをDNSサーバ３ｂに送信する（１６０）。

【００３９】DNSサーバ３ｂは、名前hostBに対するIPv4アドレス“ｂ”を応答する（１６１）。トランスレータ１ａのTR-Tは、DNSのメッセージを含むパケットを検出し、パケットを変換する（１６２）。送信元アドレスに、VPN５ｂに対応する仮想プレフィックスβを付加する。着信先アドレスは、トランスレータ１ａが備えるDNS-ALGアドレス変換情報を用いて“pb4”から“β６”に変換する。トランスレータ１ａのTR-Tは、アドレスを変換したパケットをDNS-ALG２ａに送信する（１６３）。

【００４０】DNS-ALG２ａは、名前hostBに対するIPv4アドレス“ｂ”に仮想プレフィックスβを付加し、“β＋ｂ”に書き換える（１６４）。

【００４１】DNS-ALG２ａは、DNS-ALG２ａのVPN５ａ用のIPv6アドレス“α６”宛に、RDATAに“β＋ｂ”を設定したDNS応答を送信する（１６５）。

【００４２】DNS応答を受信したDNS-ALG２ａは、以後の変換のためにIPv6アドレス“β＋ｂ”を着信先仮想IPv4アドレス“ｂ`”に変換する（１６６）。このIPv4アドレスは名前host Bに対する仮想的なアドレスで、VPN５ａで使用されていないIPアドレスの集合から選ぶ。

【００４３】DNS-ALG２ａは、DNSサーバ３ａ経由で端末４ａに名前hostBに対する着信先仮想IPv4アドレス“ｂ`”を送信する（１６９、１７１、１７２）。トランスレータ１ａはDNS応答１６９を検出すると、パケットを変換する（１７０）。着信先アドレスから、仮想プ

レフィックスαを削除する。送信元アドレスは、トランスレータ１ａが備えるDNS-ALGアドレス変換情報を用いて“α６”から“pa4”からに変換する。トランスレータ１ａのTR-Oは、アドレスを変換したパケットをDNS３ａに送信する（１７１）。

【００４４】DNS-ALG２ａは、“β＋ｂ”と“ｂ’”の対応付け変換規則を作成し、トランスレータ１ａに送信する（１６７）。トランスレータ１ａは、変換規則を変換情報記憶部１１のVPN＃１変換情報テーブル５１０に記憶し、DNS-ALG２ａに応答を送信する（１６８）。

【００４５】図１５と図１８の主な差分は、「トランスレータ１は、着信先アドレスと送信元アドレスの変換を行い（１８２）、パケットをトランスレータ内でルーティングし（１８４）、再び着信先アドレスと送信元アドレスの変換を行う（１８５）」ことである。

【００４６】端末４ａは端末４ｂへ向けてIPパケットの送信を始める。これらのパケットの着信先アドレスはｂ’、送信元アドレスは端末のIPv4アドレスａである（１８１）。

【００４７】トランスレータ１ａは、このパケットが到着するとデータパケット変換・処理部１３に送る。ここでは、変換情報記憶部１１にデータを受信した回線の番号と着信先アドレスb’で検索をかける。すると、ステップ１６７で準備したエントリが変換情報テーブル５１０に見つかるため、着信先アドレスを“ｂ’”を“β＋ｂ”に変換する。送信元アドレスには、データを受信した回線番号に対応する仮想的なIPv6プレフィックスαを付加する（１８２）。

【００４８】トランスレータ１ａは着信先アドレスに“β＋ｂ”、送信元アドレスに“α＋ａ”を設定したパケットを送信する（１８３）。このパケットは、トランスレータ１ａ内でルーティングされる（１８４）。

【００４９】トランスレータ１ａは、このパケットをデータパケット変換・処理部１３に送る。ここでは、着信先アドレスから仮想IPv6プレフィックスβを削除する。トランスレータ１ａは、送信元アドレス“α＋ａ”をIPv4アドレス“ａ’”に変換する。このIPv4アドレスは、IPv6アドレス“α＋ａ”に対する仮想的なアドレスで、VPN５ｂで使用されていないIPアドレスの集合から選ぶ。

【００５０】トランスレータ１ａは、“α＋ａ”と“ａ’”の対応付け変換規則を作成し、変換情報記憶部１１のVPN＃２変換情報テーブル５２０に記憶する（１８５）。

【００５１】端末４ｂは、着信先アドレスに“ｂ”、送信元アドレスに“ａ’”を設定したパケットを受信する（１８６）。

【００５２】端末４ｂは、端末４ａへ向けて着信先アドレス“ａ’”、送信元アドレス“ｂ”を設定したパケットを送信する（１８７）。

【００５３】トランスレータ１ａはこのパケットが到着するとデータパケット変換・処理部１３に送る。ここで、変換情報記憶部１１にデータを受信した回線の番号と着信先アドレス“ａ’”で検索をかける。すると、ステップ１８５で準備したエントリが変換情報テーブル５２０に見つかるため、着信先アドレス“ａ’”を“α＋ａ”に変換する。送信元アドレスには、データを受信した回線番号に対応する仮想的なIPv6プレフィックス“β”を付加する（１８８）。

【００５４】トランスレータ１ａは着信先アドレスに“α＋ａ”、送信元アドレスに“β＋ｂ”を設定したパケットをトランスレータ１ａ内でルーティングする（１８９、１９０）。

【００５５】トランスレータ１ａは、このパケットをデータパケット変換・処理部１３に送る。着信先アドレス“α＋ａ”から仮想IPv6プレフィックスαを削除する。ここで、変換情報記憶部１１に着信先の仮想IPv6プレフィックスαと送信元アドレス“β＋ｂ”で検索をかけると、さきに準備したエントリが変換情報テーブル５１０に見つかるため、送信元アドレスを“β＋ｂ”から“ｂ’”に変換する（１９１）。

【００５６】端末４ａは着信先アドレスに“ａ”、送信元アドレスに“ｂ’”を設定したパケットを受信する（１９２）。

【００５７】本発明の実施の形態によれば、トランスレータとDNS-ALGの連携と、仮想IPv6プレフィックスの活用により、複数のVPNが接続されているトランスレータはアドレスが重複する場合であっても、プライベートIPv4アドレスを有する端末を一意に識別できる。従って、プライベートIPv4アドレスを有するVPN間で相互通信が可能になる。

【００５８】また、VPN毎のDNS-ALGを１つの物理装置に縮退することにより、VPN間でDNS-ALG装置を共有することが可能になる。

【００５９】本発明の第３の実施の形態を図面を用いて説明する。

【００６０】図１９は、本発明の第３の実施例の網構成を示す。図１６と比較すると、本実施例は、「複数のVPNがDNS-ALGを共有する」ことと、「複数のトランスレータがDNS-ALGを共有する」ことを特徴とする。本実施例におけるDNS-ALG２ａは、ドメイン毎に名前解決の転送先を別々に設定する機能を備える。具体的には、次に問い合わせるDNSサーバのアドレス情報として、各VPNのドメイン名とそのVPNに存在するDNSサーバの仮想IPv6アドレスの対応関係を管理する。この仮想IPv６アドレスは、“仮想プレフィックス＋各VPNにおいて、DNSサーバに割り当てられたIPv4アドレス”で構成する。

【００６１】DNS-ALG２ａは、処理ルーチン６０のかわりに、名前hostBのQTYPEの値にかかわらず、“A”及び”AAAA”で名前解決を行う機能を備える。本実施例におけるトランスレータ１は、実施例１におけるトランス

レータ１の機能に加え、DNS-ALGアドレス変換情報と、DNSのメッセージを含むパケットを監視する機能と、DNSのメッセージを含むパケットのアドレス変換機能を備える。

【００６２】DNS-ALGアドレス変換情報は、DNS-ALGのIPv6アドレスとVPNの内部でDNS-ALGを識別するためDNS-ALGに割り当てられた仮想IPv4アドレスとの対応関係を管理する。

【００６３】以下、VPN５ａに存在する端末４ａがVPN５ｂに存在する端末４ｂの名前を解決する場合について説明する。

【００６４】本実施例において、トランスレータ１ａはDNS-ALG2aのIPv6アドレス“alg6”とVPN毎にVPNの内部でDNS-ALGを識別するためにDNS-ALG２ａに割り当てられた仮想IPv6の対応関係を保持する。

【００６５】端末４ａは端末４ｂの名前(host Ｂとする)のアドレスを得るためにDNS問い合わせを行う。DNSサーバ３ａは名前hostBを解決できないため、次のDNSサーバ（DNS-ALG2a）にDNS問い合わせを送信する。このDNS問い合わせのパケットヘッダの着信先アドレスにはDNS-ALG２ａに対してVPN５ａで割り当てられた仮想IPv4アドレス“ｐａ4”が、送信元アドレスにはDNS３ａのIPv4アドレス”da4”が設定される。

【００６６】トランスレータ１ａがこのDNS問い合わせを検出すると、DNS-ALGアドレス変換情報を参照して着信先アドレスを“pa４”からDNS-ALG2aのIPv6アドレス“alg6”に変換する。送信元アドレスには、VPN5a用のIPv6プレフィックスαを付加し、“α＋da4”に書きかえる。

【００６７】上記DNS問い合わせを受信したDNS-ALG２ａは、名前host Ｂに対するIPアドレスを知らない場合、次のDNSサーバに問い合わせる。ここで、名前hostBを解決するために、次に問い合わせるべきDNSサーバとして、仮想IPv6アドレス“β+db４”が設定される。“β+db４”は、VPN５ｂのDNSサーバ３ｂの仮想IPv6アドレスである。

【００６８】DNS-ALG２ａは、DNS問い合わせをDNSサーバ３ｂに送信し、応答を待つ。このDNS問い合わせの送信元アドレスにはDNS-ALG2aのIPv6アドレス“alg6”が、着信先アドレスには“β+db４”が設定される。

【００６９】トランスレータ１ａは、上記DNS問い合わせのパケットを検出し、VPN毎のDNS-ALGアドレス変換情報を用いて送信元アドレスを、DNS-ALG2aのIPv6アドレス“alg6”をVPN5b内でDNS-ALG2aを識別する仮想IPv4アドレス“pb4”に変換する。着信先アドレスはプレフィックスβを削除し、“β+db４”から“db４”に書き換える。

【００７０】DNSサーバ３ｂは、DNS-ALG２ａに、名前hostBに対するIPv4アドレス“ｂ”を応答する。

【００７１】DNS-ALG２ａは、以後の変換のためにIPv4アドレス“ｂ”を着信先仮想IPv6アドレス“β＋ｂ”に書き換えたのち、“β＋ｂ”を着信先仮想IPv4アドレス“ｂ’”に変換する。上記IPv4アドレス“ｂ’”は名前host Ｂに対する仮想的なアドレスで、VPN５ａで使用されていないIPアドレスの集合から選ぶ。

【００７２】DNS-ALG２ａは、DNSサーバ３ａ経由で端末４ａに名前hostBに対する着信先仮想IPv4アドレス“ｂ’”を送信する。

【００７３】以降の処理の流れは、第２の実施例と同じである。

【００７４】本発明の実施の形態によれば、DNS-ALG がマルチホームノードでない場合であっても、VPN間でDNS-ALGを共用でき、さらにDNS-ALGにおける処理を軽減できる。

【００７５】本発明の第４の実施の形態を図面を用いて説明する。

【００７６】図２０は、本発明の第４の実施例の網構成を示す。図１６と比較すると、図２０の網構成は、「L2SW７がVPN5毎に存在するトランスレータの回線（17a、17b）を多重する」ことを特徴とする。本実施例におけるL2SW７は、図２１に示すVPN管理テーブル３２０を備える。

【００７７】図２１は、VPN管理テーブル３２０のテーブル構成を示す。本テーブルは、MACアドレスやIEEE 802.1QのTAG IDに代表されるレイヤ２（L2）情報毎に生成された複数のエントリ（３２０－１～３２０－ｎ）からなる。各エントリは、L2情報３２１対応に、VPN識別子３２２と、対トランスレータの回線番号３２３を定義する。

【００７８】本実施例において、VPN５ａからパケットを受信したL2SW７は、VPN管理テーブル３２０を受信パケットのL2情報（例えば、送信元MACアドレスや、IEEE 802.1QのTAG ID）で検索する。L2SW７は、VPN5aに対応する回線１７ａからトランスレータ１ａにパケットを送信する。

【００７９】本発明の実施の形態によれば、トランスレータが回線対応に収容するVPNをL2SWで多重することができる。

【００８０】本発明の第５の実施の形態を図面を用いて説明する。

【００８１】図２２は、本発明の第５の実施例の網構成を示す。図１６と比較すると、図２２の網構成は、「トランスレータ１ａの回線17aに複数のVPN（5a、5b）が収容される」ことと、「トランスレータ１ａが図９に示す仮想プレフィックス管理テーブル３００のかわりに図１０に示す仮想プレフィックス管理テーブル３１０を備え、L2情報からVPNを識別する」ことを特徴とする。

【００８２】図１０は、仮想プレフィックス管理テーブル３１０のテーブル構成を示す。本テーブルは、MACアドレスやIEEE 802.1QのTAG IDに代表されるレイヤ２（L

2）情報毎に生成された複数のエントリ（３１０－１～３１０－ｎ）からなる。各エントリは、L2情報３１１対応に、VPN識別子３１２と、仮想プレフィックス３１３を定義する。

【００８３】本実施例において、VPN５ａからパケットを受信したトランスレータ１ａは、仮想プレフィックス管理テーブル３１０を受信パケットのL2情報（例えば、送信元MACアドレスやIEEE 802.1Q TAG ID）で検索する。すると、L2情報に対応する仮想プレフィックスαが仮想プレフィックス管理テーブル３１０に見つかる。トランスレータ１ａは、仮想プレフィックスによりVPNを識別する。

【００８４】本発明の実施の形態によれば、トランスレータの１つの回線に複数のVPNを収容できる。

【００８５】

【発明の効果】以上の実施の形態から明らかなように、本発明はIPv6ベースのDNS-ALGとトランスレータの連携によって、従来のTwice NATによるアドレス変換で必要な変換情報を動的に作成する場合に必要であった、着側の端末に対する仮想アドレスを生成するDNS-ALGの処理負荷の軽減と大容量変換テーブルの削減を可能にする。

【００８６】本発明によるトランスレータとDNS-ALGをプロバイダが一括管理し、トランスレータに複数のVPNを収容すれば、既存のVPNを置きかえることなく、VPN間の相互接続が可能になる。

【図面の簡単な説明】

【図1】本発明の第１の実施例であるIP網を介したVPNの相互接続構成を示すブロック図。

【図2】トランスレータ１の一例のブロック図。

【図3】DNS-ALG2の一例のブロック図。

【図4】IPv4パケットのフォーマット図。

【図5】IPv6パケットのフォーマット図。

【図6】DNS問い合わせのフォーマット図。

【図7】DNS応答のフォーマット図。

【図8】DNS応答の詳細フォーマット図。

【図9】トランスレータ１が備える仮想プレフィックス管理テーブルのテーブル図。

【図10】本発明の第５の実施例において、トランスレータ１が備える仮想プレフィックス管理テーブルのテーブル図。

【図11】トランスレータ１が備える変換情報テーブルのテーブル図。

【図12】DNS-ALG２が備えるDNSメッセージ変換処理ルーチンの流れ図。

【図13】DNS-ALG２が備えるDNSメッセージ変換処理ルーチンの流れ図。

【図14】本発明の第１の実施例における名前解決のシーケンス図。

【図15】本発明の第１の実施例におけるVPNが相互通信する場合のシーケンス図。

【図16】本発明の第２の実施例であるトランスレータに複数のVPNが接続される場合の網構成を示すブロック図。

【図17】本発明の第２の実施例における名前解決のシーケンス図。

【図18】本発明の第２の実施例におけるVPNが相互通信する場合のシーケンス図。

【図19】本発明の第３の実施例である複数のVPNが１つのDNS-ALG装置を利用する場合の網構成を示すブロック図。

【図20】本発明の第４の実施例であるL2SW７がVPNを多重する場合の網構成を示すブロック図。

【図21】本発明の第４の実施例において、L2SW７が備えるVPN管理テーブルのテーブル図。

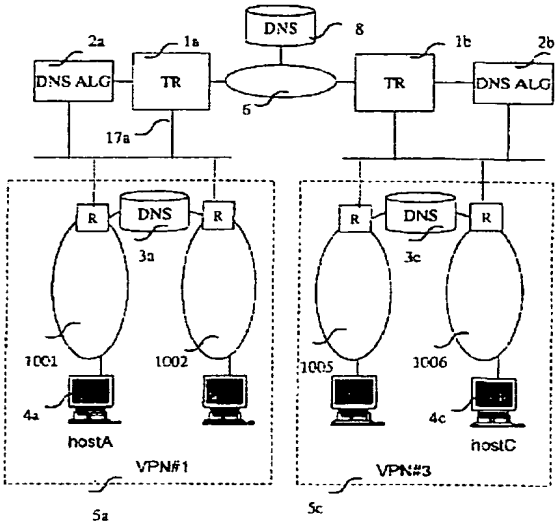
【図22】本発明の第５の実施例であるトランスレータ１がL2情報を活用してVPNを識別する場合の網構成を示すブロック図。

【符号の説明】

1 トランスレータ、2 DNS-ALG、3 VPN5が備えるDNSサーバ、4 VPNの端末、5 VPN、6 IP網、7 L2SW、8 IP網6が備えるDNSサーバ、31 送信元IPv4アドレス、32 着信先IPv4アドレス、33 IPv4ペイロード、34 送信元IPv6アドレス、35 着信先IPv6アドレス、36 IPv6ペイロード、41 DNSメッセージヘッダ部、42 DNS問い合わせ部、43 DNS応答部、60 DNS変換処理ルーチン。

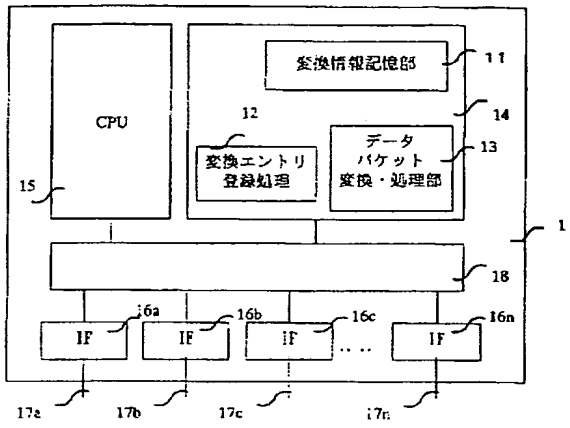
【図１】

図1



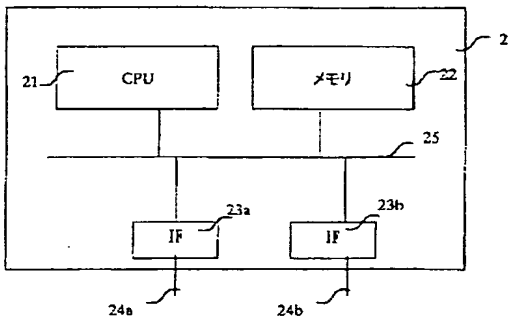
【図２】

図2



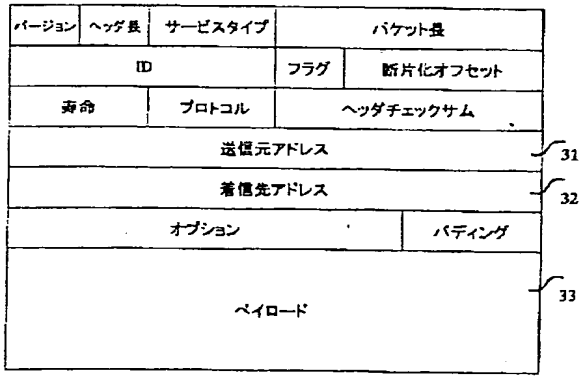
【図３】

図3



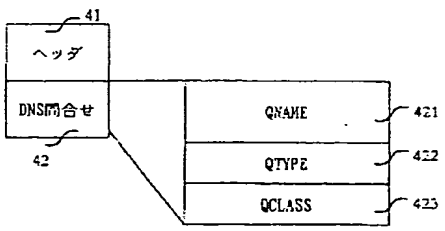
【図４】

図4



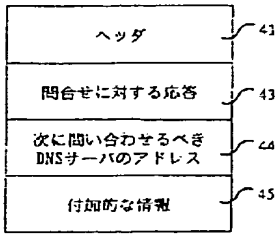
【図６】

図6



【図７】

図7



【図９】

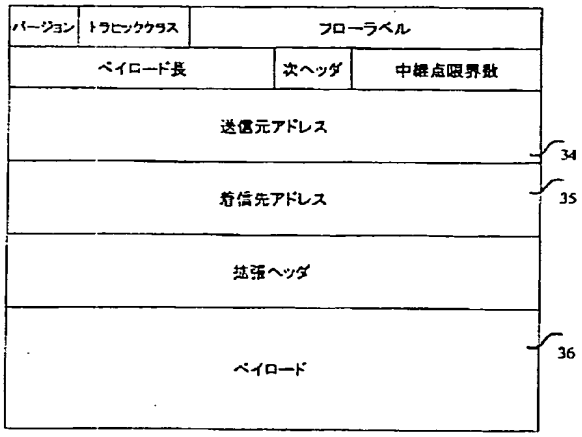
図9

300 仮想プレフィックス管理テーブル

301 回線番号	302 仮想プレフィックス	303 ポインタ	
xxx	α	p1	300-1
xxy	β	p2	300-2
⋮			300-n

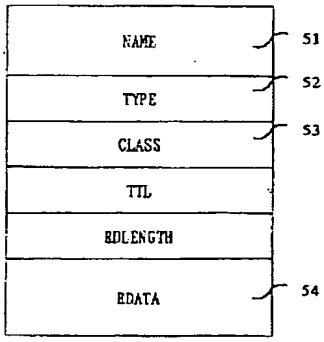
【図５】

図5



【図８】

図8



【図１０】

図10

310 仮想プレフィックス管理テーブル

311 L2情報	312 VPN識別子	313 仮想プレフィックス	
aaa	1	α	310-1
bbb	2	β	310-2
⋮			310-n

【図１１】

図11

500 変換情報テーブル

510 VPN#1 変換情報テーブル

501 V4アドレス	502 V6アドレス	
b'	β + b	510-1
c'	γ + c	510-2
⋮		510-n

520 VPN#2 変換情報テーブル

501 V4アドレス	502 V6アドレス	
a'	α + a	520-1
⋮		520-n

530 VPN#3変換情報テーブル

501 V4アドレス	502 V6アドレス	
a1'	α + a	530-1
⋮		530-n

【図２１】

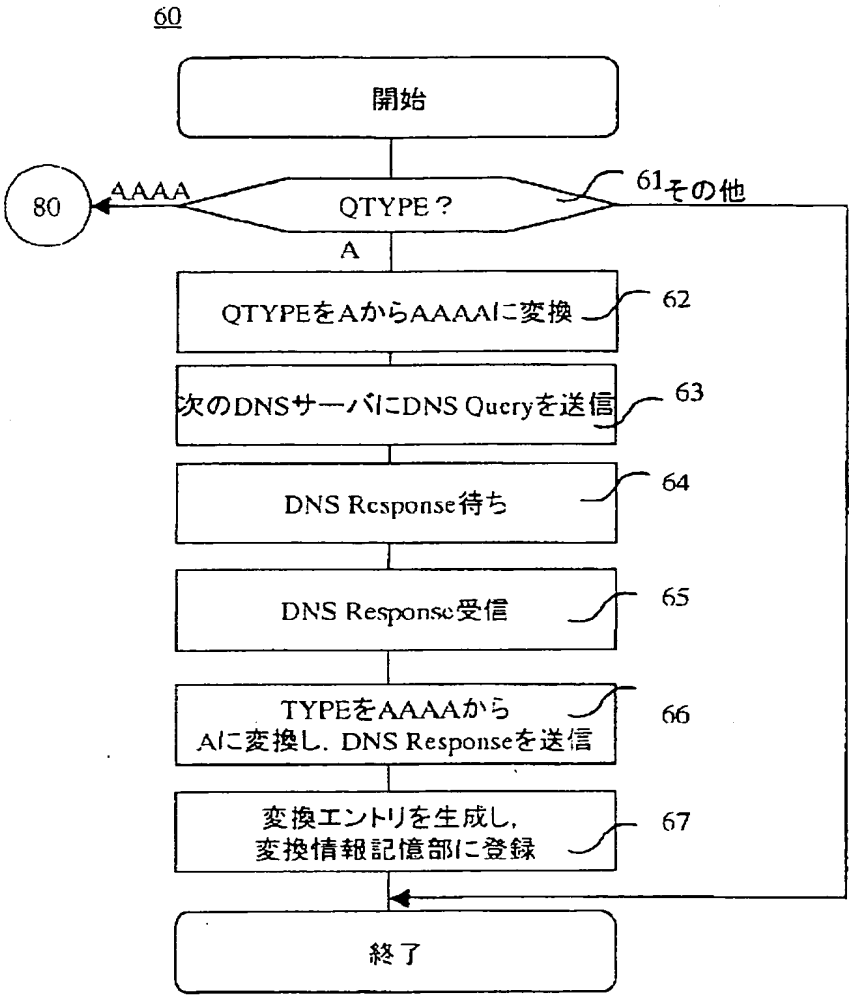
図21

320 VPN管理テーブル

321 L2情報	322 VPN識別子	323 回線番号	
aaa	1	xxx	320-1
bbb	2	yyy	320-2
⋮			320-n

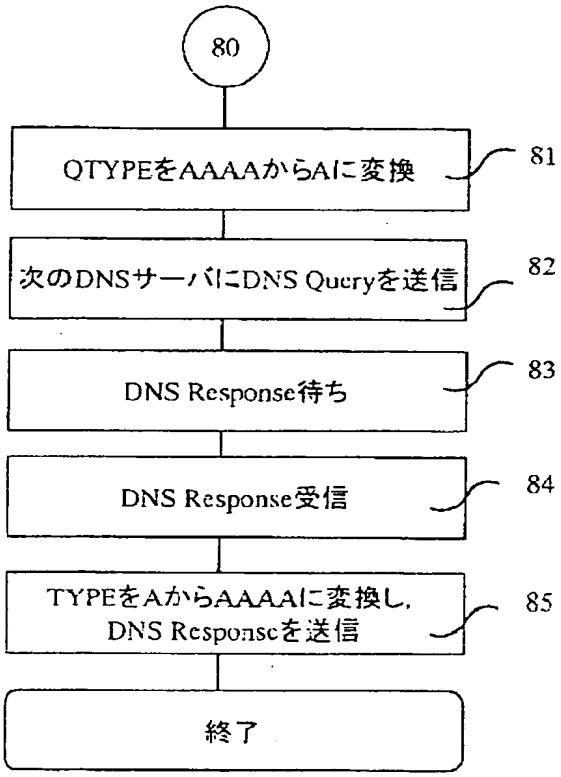
【図１２】

図12


60
開始
80
AAAA
QTYPE？
61
その他
A
QTYPEをAからAAAAに変換
62
次のDNSサーバにDNS Queryを送信
63
DNS Response待ち
64
DNS Response受信
65
TYPEをAAAAから
Aに変換し，DNS Responseを送信
66
変換エントリを生成し，
変換情報記憶部に登録
67
終了

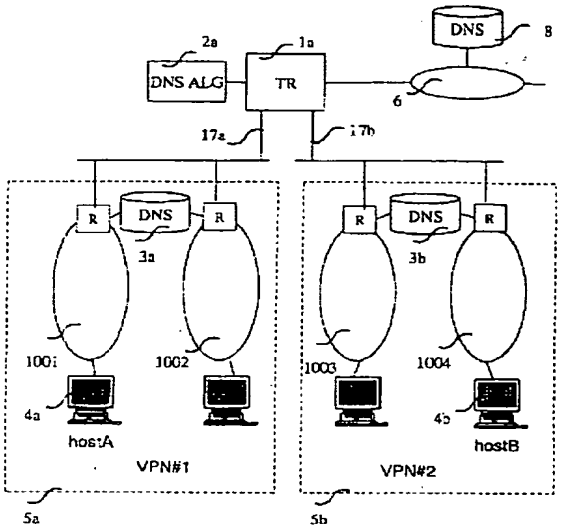
【図１３】

図13



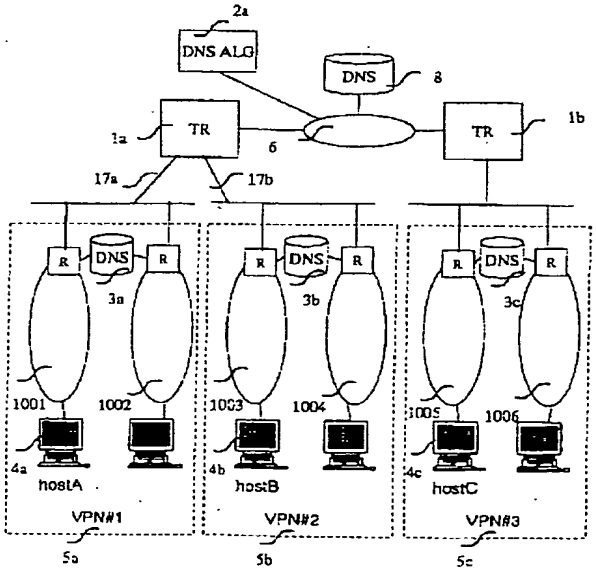
【図１６】

図16



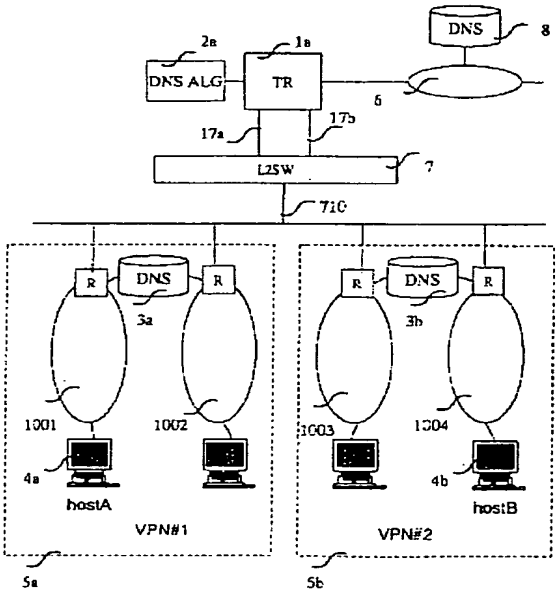
【図１９】

図19



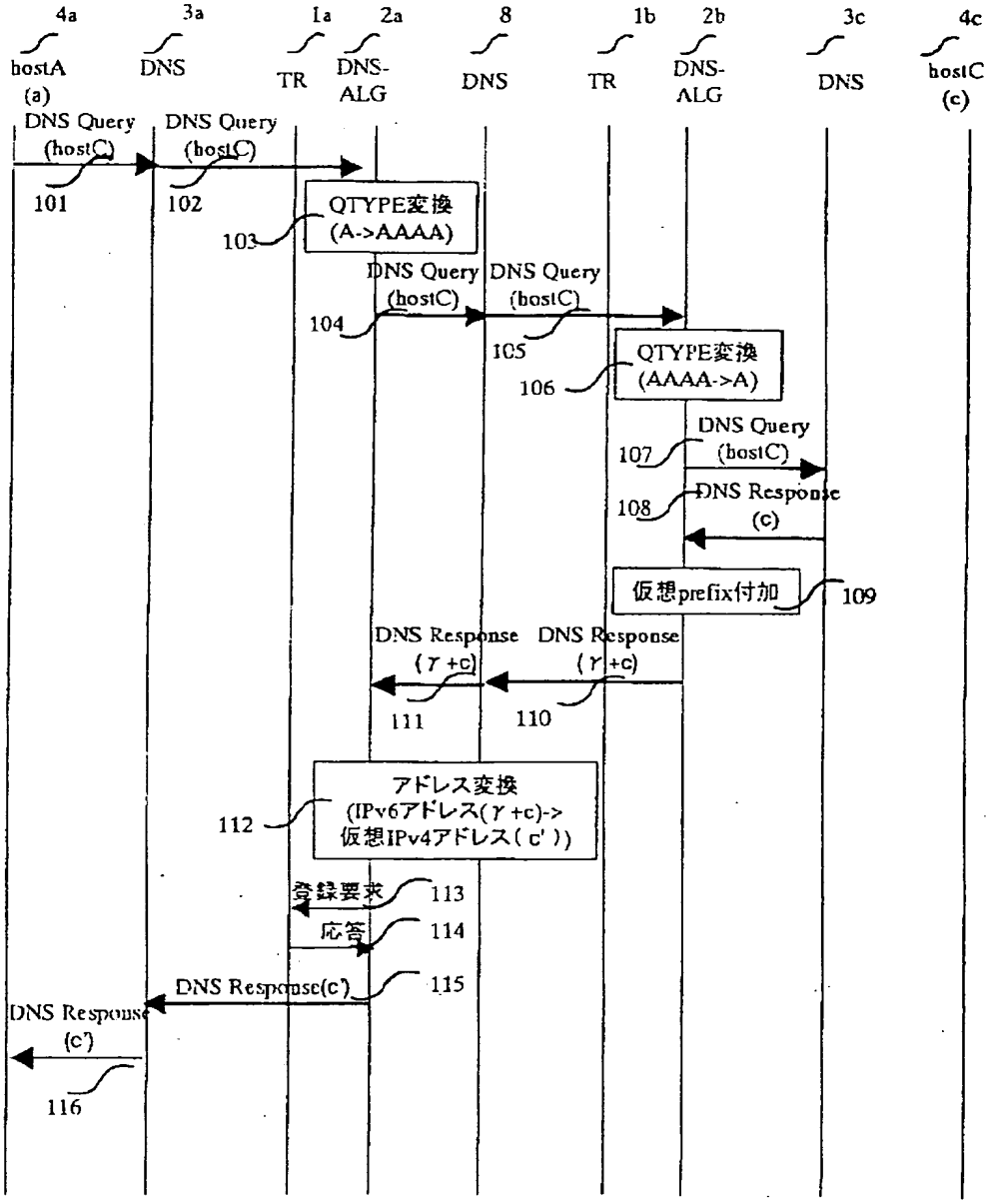
【図２０】

図20



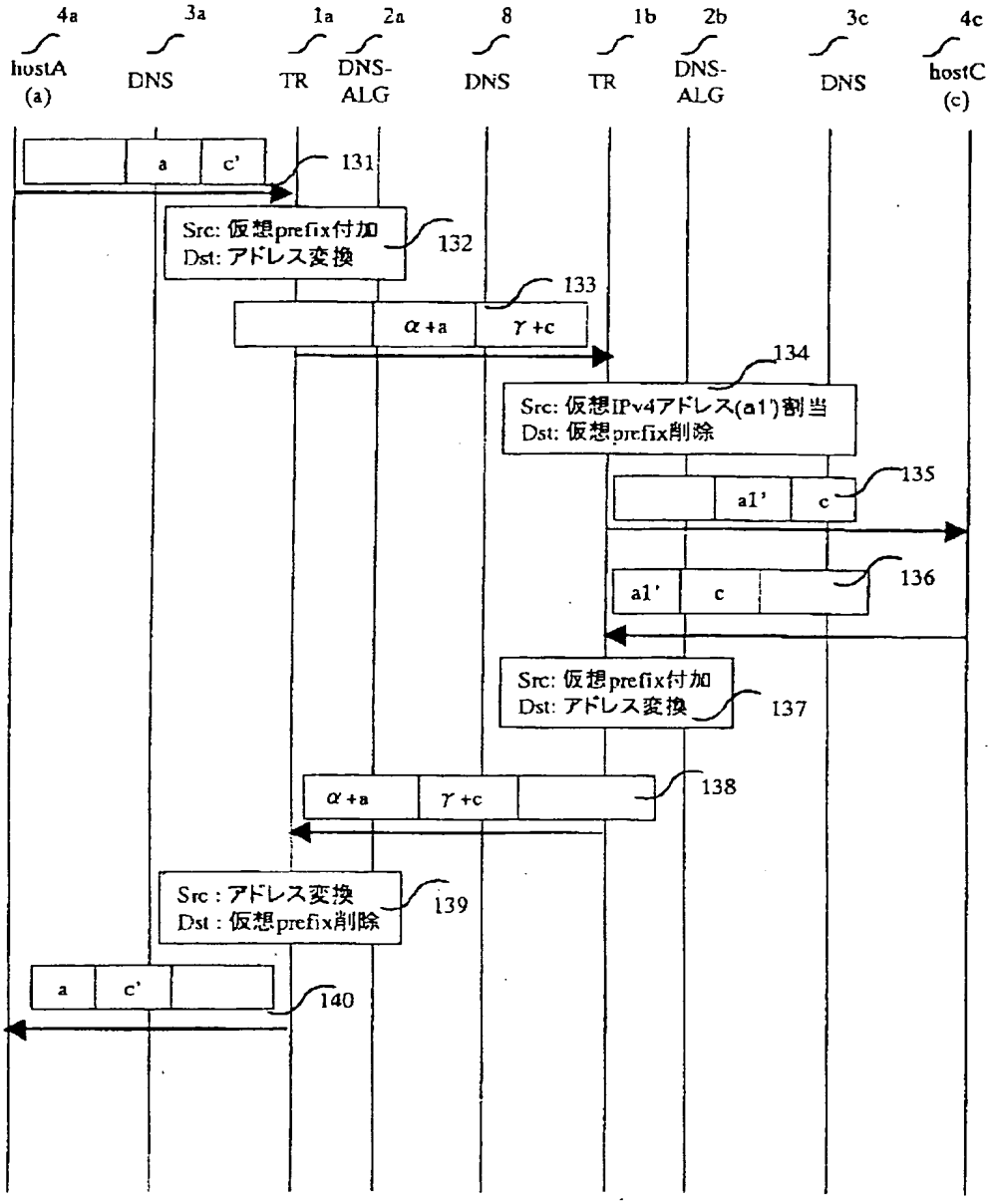
【図１４】

図14


4a
hostA
(a)
3a
DNS
1a
TR
2a
DNS-
ALG
8
DNS
1b
TR
2b
DNS-
ALG
3c
DNS
4c
hostC
(c)
DNS Query
(hostC)
101
DNS Query
(hostC)
102
QTYPE変換
(A->AAAA)
103
DNS Query
(hostC)
104
DNS Query
(hostC)
105
QTYPE変換
(AAAA->A)
106
DNS Query
(hostC)
107
DNS Response
(c)
108
仮想prefix付加
109
DNS Response
(γ+c)
111
DNS Response
(γ+c)
110
アドレス変換
(IPv6アドレス(γ+c)->
仮想IPv4アドレス(c'))
112
登録要求
113
応答
114
DNS Response(c')
115
DNS Response
(c')
116

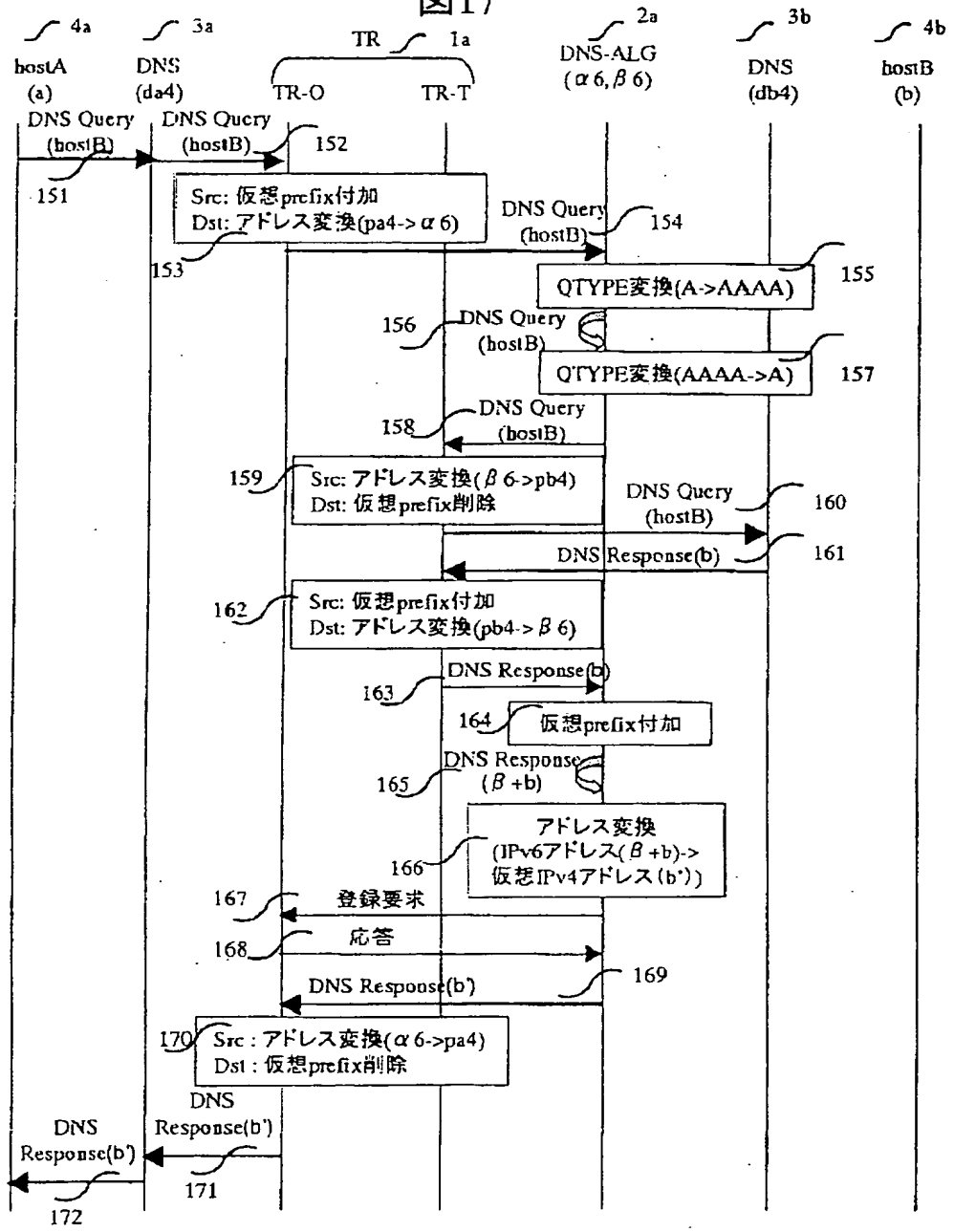
【図１５】

図15


4a
hostA
(a)
3a
DNS
1a
TR
2a
DNS-
ALG
8
DNS
1b
TR
2b
DNS-
ALG
3c
DNS
4c
hostC
(c)
a
c'
131
Src: 仮想prefix付加
Dst: アドレス変換
132
133
α+a
γ+c
134
Src: 仮想IPv4アドレス(a1')割当
Dst: 仮想prefix削除
135
a1'
c
136
a1'
c
Src: 仮想prefix付加
Dst: アドレス変換
137
α+a
γ+c
138
Src : アドレス変換
Dst : 仮想prefix削除
139
a
c'
140

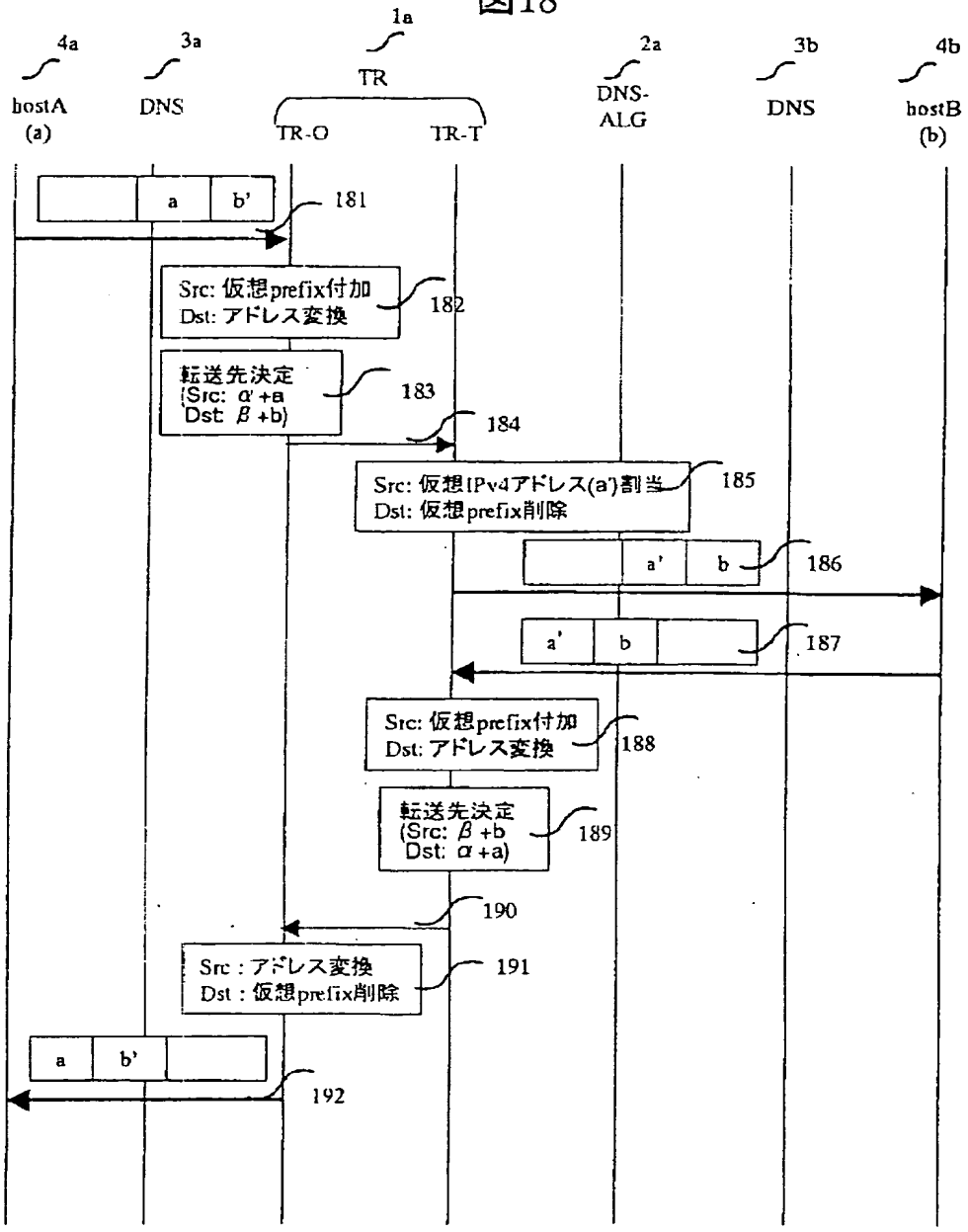
【図１７】

図17


4a
hostA
(a)
3a
DNS
(da4)
TR
1a
TR-O
TR-T
2a
DNS-ALG
(α6,β6)
3b
DNS
(db4)
4b
hostB
(b)
DNS Query
(hostB)
151
DNS Query
(hostB)
152
Src: 仮想prefix付加
Dst: アドレス変換(pa4->α6)
153
DNS Query
(hostB)
154
QTYPE変換(A->AAAA)
155
156
DNS Query
(hostB)
QTYPE変換(AAAA->A)
157
158
DNS Query
(hostB)
159
Src: アドレス変換(β6->pb4)
Dst: 仮想prefix削除
DNS Query
(hostB)
160
DNS Response(b)
161
162
Src: 仮想prefix付加
Dst: アドレス変換(pb4->β6)
DNS Response(b)
163
164
仮想prefix付加
DNS Response
(β+b)
165
アドレス変換
(IPv6アドレス(β+b)->
仮想IPv4アドレス(b'))
166
167
登録要求
168
応答
DNS Response(b')
169
170
Src : アドレス変換(α6->pa4)
Dst : 仮想prefix削除
DNS
Response(b')
171
DNS
Response(b')
172

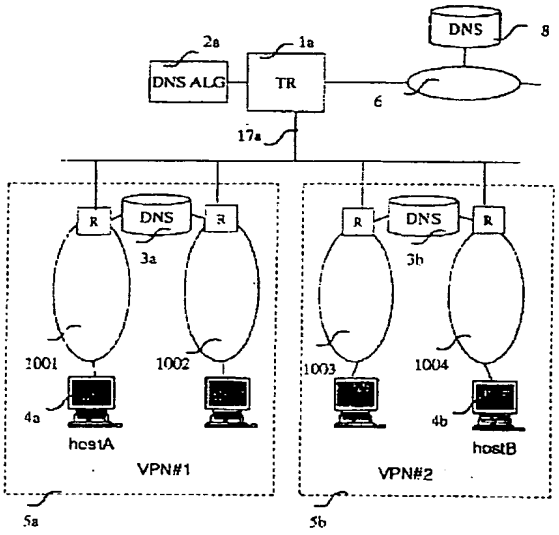
【図１８】

図18


4a
hostA
(a)
3a
DNS
1a
TR
TR-O
TR-T
2a
DNS-
ALG
3b
DNS
4b
hostB
(b)
a
b'
181
Src: 仮想prefix付加
Dst: アドレス変換
182
転送先決定
(Src: α'+a
Dst: β+b)
183
184
Src: 仮想IPv4アドレス(a')割当
Dst: 仮想prefix削除
185
a'
b
186
a'
b
187
Src: 仮想prefix付加
Dst: アドレス変換
188
転送先決定
(Src: β+b
Dst: α'+a)
189
190
Src : アドレス変換
Dst : 仮想prefix削除
191
a
b'
192

【図２２】

図22



フロントページの続き

(72)発明者　林　匡哉
東京都国分寺市東恋ケ窪一丁目280番地
株式会社日立製作所中央研究所内
(72)発明者　竹内　敬亮
東京都国分寺市東恋ケ窪一丁目280番地
株式会社日立製作所中央研究所内
(72)発明者　妹尾　高光
神奈川県横浜市戸塚区戸塚町216番地　株式会社日立製作所通信事業部内

Ｆターム(参考)　5B089 GA31 GB01 KB06 KF05 KH03
5K030 GA14 HA08 HB21 HC01 HC13
HD03 JA11 JT03 KA04 LB13
LE02 MD08 MD10
5K034 AA10 AA20 DD03 EE10 HH61